#2

PCT/CN 00/00100

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　　请　　日：99 06 02

4

申　　请　　号：99 1 07920.5

申 请 类 别：发　明

发明创造名称：一种保证计算机网络信息安全的系统及其相应的方法

发明人或设计人：余鲲

申　　请　　人：余鲲

中华人民共和国
国家知识产权局局长　姜颖

2000 年 05 月 08 日

权 利 要 求 书

1、一种保证计算机网络信息安全的计算机网络系统，包括：路由器、计算机、计算机局域网，以及密级不同且相互间在物理上隔离的计算机网络，其特征在于它还包括：

网络选择器，与所述计算机相连，用于接收用户参数，接收接通某个密级的计算机网络的请求，并对所述计算机的硬盘进行控制；

安全集线器，连接在所述网络选择器和所述计算机局域网的集线器之间，用于响应网络选择器的请求，根据来自网络选择器的用户参数和请求，对使用计算机的用户的合法性进行判断，并依据判断结果，同意或拒绝用户访问某个密级的计算机网络的请求；

2、如权利要求 1 所述的计算机网络系统，其特征在于：所述的网络选择器和所述的安全集线器之间采用 RJ45 接口通过双绞线相连、并且用 RJ45 中的两对未定义的双绞线中的一对双绞线来传递所述用户参数、请求和控制信息。

3、如权利要求 1 中所述的计算机网络系统，其特征在于：所述的计算机是无硬盘计算机或有硬盘计算机。

4、如权利要求 2 所述的计算机网络系统，其特征在于：所述的网络选择器带有 IC 卡的驱动器，用于读出 IC 卡中存贮的用户信息。

5、如权利要求 2 所述的计算机网络系统，其特征在于：所述的安全集线器带有读 IC 卡的驱动器，安全集线器识别系统管理员的身份卡，生成用户身份卡。

6、如权利要求 1，2，3，4，5 任意之一所述的计算机网络系统，其特征在于：所述的网络选择器置于计算机内部，网络选择器的面板成为计算机面板的组成部分。

7、如权利要求 1 所述的计算机网络系统，其特征在于：它还包括：

层联集线器，所述层联集线器双侧采用 RJ45 接口，连接于所述网络选择器与所述安全集线器之间，并且用 RJ45 中的两对未定义的双绞线中

[redacted]双绞线来传递所述用户参数、请求和控制信息，用于将更多的计算机和网络选择器接入安全集线器。

8、一种用于保证计算机网络信息安全的方法，包括以下步骤：

(1)接收用户参数，并提出接通某个密级的计算机网络的请求；

(2)响应所述接通某个密级的网络的请求，根据所述用户参数对用户合法性进行判断；

(3)依据判断结果，同意或拒绝用户接通某个密级的计算机网络的请求。

9、如权利要求 8 所述的方法，其特征在于接收用户参数的步骤包括以下步骤：

获取用户身份，密钥，用户访问网络密级的权限，用户当前所要访问的计算机网络的号码，是否要求从网络启动本地计算机，是否有系统盘等参数。

10、如权利要求 8 所述的方法，其特征在于所述响应所述接通某个密级的网络的请求的步骤还包括下列步骤：

(1)判断该用户是否访问有密级的网络；

(2)若所述用户不访问有密级的网络，则为用户接通互联网；

(3)若所述用户访问有密级的网络，则判断该用户是否有权使用该网络。

说　明　书

一种保证计算机网络信息安全的系统及其相应的方法

本发明涉及计算机网络的信息安全，具体地是在以太网络上加入网络选择器和安全集线器就可以使用一台计算机访问到多个不同密级且相互间在物理上隔离的计算机网络。

互联网络是把计算机局域网络连接在一起并运行 IP 协议的计算机网络。为保证计算机网络的信息安全，通常的方法是在局域网络和互联网络之间加入防火墙或代理服务器，通过软件方法控制从互联网络对局域网络的访问。但是，这并没有使得连入互联网络的计算机免遭来自互连网络的攻击。因此那些有价值的、保密的信息得不到安全保证。

为了保证信息安全，现在通常采用物理网络隔开的方法，也就是保证互联网络与有价值的、保密的内部计算机网络在物理线路上没有连接。这样办公室内部就要进行两个网络的布线施工，办公桌上要摆放两个计算机，不仅增加了办公信息系统的成本，也给信息系统的使用带来不便。如果需要再增加几个不同密级的计算机网络的话，就需要在办公室中再增加若干台计算机，效果也不会理想。

本发明的目的旨在提供一种计算机网络信息安全的方法及基于该方案的实现计算机网络信息安全的网络系统，以解决计算机网络的信息安全性和计算机网络的可用性之间的矛盾，克服目前计算机网络信息不安全的缺点。

本发明的一个方案是提供了一种保证计算机网络信息安全的计算机网络系统，包括：路由器，计算机，计算机局域网，以及密级不同且相互间在物理上隔离的计算机网络，其特征在于它还包括：

网络选择器，与所述计算机相连，用于接收用户参数，接收接通某个密级的计算机网络的请求，并对所述计算机的硬盘进行控制；

安全集线器，连接在所述网络选择器和所述计算机局域网的集线器之

于响应网络选择器的请求，根据来自网络选择器的用户参数和请求，对使用计算机的用户的合法性进行判断，并依据判断结果，同意或拒绝用户访问某个密级的计算机网络的请求。

本发明的第二方案是提供一种用于保证计算机网络信息安全的方法，包括以下步骤；

(1)接收用户参数，并提出接通某个密级的计算机网络的请求；

(2)响应所述接通某个密级的计算机网络的请求，根据所述用户参数对用户的合法性进行判断；

(3)依据判断结果，同意或拒绝用户访问某个密级的计算机网络的请求。

本发明实现计算机网络信息安全的方法主要是对现有的树型计算机网络的传输末端加以改造，无需改变已有网络的布线系统，整个计算机网络的物理变动较小，且成本低，时间短，容易成功。

过去要建安全的计算机信息网络必须把内部计算机网络和互联网络物理隔离，也就是要建两个完全并行的计算机网络系统。本发明实现计算机网络信息安全的方法只需一套以太网络，减少了网络的复杂度和建设成本。

用户在一台计算机上可以访问到多个计算机网络，方便快捷，有利于提高工作效率。由于无盘计算机相对简单，用户对计算机系统的维护省时、省力。

由于本发明实现计算机网络信息安全的技术方案和实现方法允许密级的分类个数随意增减，因此它不仅适用于组织规模不大，保密要求不高，只需要两个物理隔离的计算机网络就够了的机构，还适用于跨地区、跨国界、员工数量多、业务流程复杂、计算机网络信息的安全敏感性强、密级分得细的机构，尤其是政府机关、跨国公司等。

计算机经过集中计算、分布计算和网络计算的发展历程，目前正处于网络计算阶段。集中计算就是用户通过计算机终端使用大型计算机上的信

分布计算就是大中小计算机保存各自的数据，各计算机各算各自的，联网共享信息，弱化了主机的地位；网络计算就是数据统一存储在大型计算机上，但数据处理可以在联网的网络计算机上进行，即数据分布计算，信息集中管理。本发明实现计算机网络信息安全的方法及基于此方法的实现计算机网络信息安全的网络系统正是符合这种趋势，有利于用户的计算机网络长期使用。

图 1 是根据本发明的网络选择器的构形图；

图 2 是根据本发明的安全集线器的构形图；

图 3 是根据本发明的 RJ45 Plus 插头的构形图；

图 4 是传统的物理隔离的计算机网络示意图；

图 5 是根据本发明第一实施例的多个密级的计算机网络构成图；

图 6 是经典的安全计算机网络构成图；

图 7 是根据本发明对图 6 改造后的安全计算机网络构成图；

图 8 是根据本发明的保证计算机网络信息安全的网络系统流程图；

图 9 是根据本发明的系统中的网络选择器中的软件流程图；

图 10 是根据本发明的系统中的安全集线器中的软件流程图。

下面将结合附图对本发明进行详细描述。

用本发明的技术方案所设计的计算机局域网络将延用传统的树型布线系统，计算机处在树叶位置上，其网络接口标准是 RJ45，由此引出的 4 对双绞线接入计算机旁的网络选择器（图 1），该网络选择器再通过 RJ45 接口引出的 4 对双绞线接入远端的更接近树根的安全集线器（图 2），在安全集线器的另一侧有八个 RJ45 接口，分别为接入互联网络（Internet）、国内网络、外联网络（Extranet）、内联网络（Intranet）、内部网络（Innernet）、秘密网络、机密网络和绝密网络。这八个计算机网络都安装了为无盘计算机工作的文件服务器，文件服务器中存有各无盘计算机的启动程序和各用户的系统数据和工作数据，此外这八个计算机网络上还分别安装有域名服务器、WWW 服务器、FTP 服务器等。

所谓无盘计算机是指该计算机本身既没有引导设备启动的系统硬盘，也没有存放数据的硬盘，而是有内存和中央处理器（CPU），此外还有主机板、主机箱、显示器、键盘等。无盘计算机只能以如上所述的网络连接方式通过以太网络读取文件服务器中的有关该计算机的引导程序到本地内存，然后再从本地内存用该程序启动有关设备。启动成功后，无盘计算机将从文件服务器上读取工作数据到本地内存进行加工，然后再存储到网络服务器上。

将互联网络（Internet）、国内网络、外联网络（Extranet）、内联网络（Intranet）、内部网络（Innernet）、秘密网络、机密网络和绝密网络预先依次编号为 0~7，网络选择器根据用户设置的编号得知用户所要接通的网络。网络选择器含有读卡机，因此，网络选择器有读取插入读卡机中的用户身份卡上的信息的功能，当不插入用户身份卡时，网络选择器自动设为0，表明任何用户都将可以访问互联网络。每台计算机都将配有一个网络选择器。

安全集线器把多个计算机分别接入由其网络选择器指定的计算机网络，安全集线器保证这八个计算机网络是相互隔离的。安全集线器之含有读卡机，只有系统管理员才能持有安全集线器的管理卡，只有系统管理员才有权维护安全集线器。系统管理员在安全集线器上设置每个用户的密级权限等信息，并为每个用户生成用户身份卡。

安全集线器的特例是层联集线器，层联集线器的网络侧的接口只有一个，而其计算机侧的接口有多个，不带IC卡，层联集线器的作用是扩大用户接入数。

由于RJ45定义了的两对双绞线用于以太网的各种协议和网络数据的传送，所以本发明使用另外两对中的一对双绞线（图3）来传送用户身份和使用网络密级的权限等信息。图3中T1、T2表示RJ45中未定义的两对双绞线中的任意一对，标在第4芯和第5芯只是示意性的。这样，各芯的定义分别是：

1--数据发送“+”

2--数据发送“-”

3--数据接收“+”

4--密级、身份证明等发送“+”

5--密级、身份证明等发送“-”

6--数据接收“-”

7--暂不用

8--暂不用

本发明把这样定义的 RJ45 称为 RJ45 Plus。因此，网络选择器的计算机侧接口是 RJ45，网络选择器的网络侧接口是 RJ45 Plus，安全集线器的计算机侧是 RJ45 Plus，安全集线器的网络侧接口是 RJ45，层联集线器的两侧接口都是 RJ45 Plus。

传统的计算机网络物理隔离方法（见图 4），使得办公桌上不得不摆两个计算机，一个接入互联网络，另一个接入内部网络。虽然安全性强，但是要两套计算机网络，成本高，占用工作桌面太大，使用不方便。

对图 4 改造以后的网络（见图 7），因为安全集线器和网络选择器的共同作用，使用户可以主动地选择将计算机连入任意一个计算机网络。因为安全集线器将两个计算机网络物理隔离，所以，图 5 既不丧失网络的物理隔离保障安全的特性，又降低了成本，节省了空间。

经典的安全计算机网络，几乎无法保密。目前对网络的保护措施大多数还是采用防火墙／代理服务器的技术模式（见图 6），但是网络黑客可以用假冒合法用户等多种手段穿过防火墙／代理服务器，进入用户的内部计算机网络。而本发明是物理网络隔离的，所以黑客进不来。

图 5 是根据本发明的多个密级的计算机网络信息安全系统构成图，参见图 5

在图五中，计算机局域网络延用树型布线系统，处在树叶位置上的是计算机，其网络接口标准是 RJ45，由此引出的 4 对双绞线接入计算机旁的

择器 5、6，网络选择器 5、6 再通过 RJ45 Plus 接入层联集线器 2、3、4，该层联集线器再通过 RJ45 Plus 接口接入另一个层联集线器，这样经过若干次接力，最后通过 RJ45 Plus 接口接入安全集线器 1。换句话说，就是在网络选择器 5、6 和安全集线器 1 之间插入多层层联集线器，形成塔状，当然也可以一个层联集线器都不使用。在安全集线器 1 的另一侧有八个 RJ45 接口，分别接入互联网络（Internet）、国内网络、外联网络（Extranet）、内联网络（Internet）、内部网络（Internet）、秘密网络、机密网络和绝密网络。这八个网络都安装了为无盘计算机工作的文件服务器，文件服务器中存有各无盘计算机的启动程序和各用户的系统数据和工作数据，此外各网络上还安装有域名服务器、WWW 服务器、FTP 服务器等。

将互联网络（Internet）、国内网络、外联网络（Extranet）、内联网络（Intranet）、内部网络（Internet）、秘密网络、机密网络和绝密网络预先依次编号为 0~7，网络选择器 5、6 根据用户设置的编号得知用户所要访问的网络。下文所称有密级的计算机网络是指编号为 1~7 的网络。网络选择器 5、6 含有读卡机，当不插入用户身份卡时，网络选择器 5、6 自动设为 0，表明任何用户都可以访问互联网络。每台计算机都将配有一个网络选择器。

在图 5 中，从本机硬盘启动的计算机 8 只允许接入互联网络。如果用户要接入有密级的计算机网络，那么网络选择器强行其从该有密级的计算机网络的文件服务器启动，并且在接入期间，硬盘将被停止供电。此时它与系统中其它部件的连接关系及工作过程与无盘计算机 7 的相同，在此不再重复。

安全集线器 1 把多个计算机分别接入由其网络选择器 5、6 指定的计算机网络，安全集线器 1 保证这八个计算机网络是相互隔离的。安全集线器 1 也含有读卡机，只有系统管理员才能持有安全集线器 1 的管理卡，只有系统管理员才有权维护安全集线器。系统管理员在安全集线器 1 上设置每个用户的密级权限等信息，并为每个用户生成用户身份卡。

图 7 是根据本发明的第二个实施例的信息安全计算机网络构成图，参见图 7。

计算机 7、8 通过 RJ45 接到网络选择器 5、6 的计算机侧接口，网络选择器 5、6 再通过 RJ45 Plus 接到安全集线器 1 的计算机侧接口，安全集线器 1 再分别与内部局域网和外部局域网连接，外部局域网经路由器与互联网络连接（见图 7 中，外部局域网及路由器简化在 Internet 中）。这里的内部局域网包括名字服务器、电子邮件服务器、WWW 服务、文件服务器等，它们是为该组织接入互联网服务的。

系统流程：对设备加电后，如果用户设定网络选择器为非零，则无盘计算机从内部局域网的文件服务器上启动，否则，与外部局域网的文件服务器连接启动。

网络选择器还可以置于计算机内部，与光盘驱动器或软盘驱动器合而为一，其网络号显示、网络号选择按钮、网络号确认按钮也可以结合到光盘驱动器或软盘的面板上，并引出两条信息号线到以太网卡的 RJ45 接口的 T1 和 T2 上或者在主板上的 RJ45 接口的 T1 和 T2 上，这样，用户就可以将计算机直接接入层联集线器或安全集线器。这一设计的好处是节省能源，方面使用，减少占地空间。

各局域网络可以接入八个计算机网络中的国内网络，国内网络通过广域通信网互相连接，就构成了国家的信息边疆。国内网络是国内公众的网络，只有拥有中国国籍的人才有权使用这一网络。

本发明实现计算机网络信息安全的方法和过程是：计算机、网络选择器和安全集线器分别加电后，用户在网络选择器上设定所要连接的计算机网络的编号；网络选择器检查插入的用户身份卡，获知用户身份、网络密级使用权限和网络编号等参数，并将这些参数做为对安全集线器的请求一并通过 RJ45 Plus 的 T1、T2 发送给安全集线器；如果网络选择器没有查到用户身份卡，则将网络编号自动设为 0，意味着该用户只访问互联网；安全集线器通过 RJ45 Plus 的 T1、T2 收到请求后，检查用户是否为合法用户，

是否有权访问其想访问的计算机网络，经确认后，为用户接通所要访问的计算机网；文件服务器确认用户请求后，发送无盘计算机的引导程序，据此无盘计算机启动，用户键入用户名和口令后，进入正常工作状态。

图 8 是根据本发明的保证计算机网络信息安全的网络系统流程图，下面对该流程做进一步说明。

步骤 A1 获取用户身份、密钥、用户访问计算机网络密级的权限、用户当前所要访问的网络号码、是否要求从网络启动本地计算机、是否有数据盘等参数，然后进入步骤 A2，如果 A2 判定是无盘计算机，则进入 A3，否则就是有盘计算机，进入 B1，如果这时有盘计算机不妨问互联网络，则（B2）网络选择器令计算机硬盘在访问期间不得工作，意味着该有盘计算机也将同无盘计算机一样启动和运行，转入 A3，如果步骤 A3 判断用户不合法，则（C1）告警，停止用户使用，并提醒用户更换参数，一旦用户更换了参数（C2）就返回到 A1，如果步骤 A3 判定用户合法，则为用户接通线路并正常运行（A4），直至用户参数发生改变（A5），返回步骤 A1。

图 8 的功能是由网络选择器 5、6 和安全集线器 1 中的软件相互配合实现的。网络选择器的主要功能就是为安全集线器提供用户的有关参数，并随时准备停止非法用户使用计算机网络。安全集线器的主要功能是判断用户的合法性，为合法用户接通计算机网络。下面结合图 9 和图 10 作进一步的说明。

在图 9 中，步骤 11 是网络选择器判断所连的计算机是否从本机启动。步骤 12 是网络选择器认定计算机有系统硬盘，为保证信息安全，网络选择器将不让计算机访问有密级的计算机网络，但允许它访问互联网络，所以步骤 14 强行设定网络编号为 0。步骤 13 表明该计算机是无盘计算机，它有权访问各个计算机网络，但要求用户插入身份识别卡，以便网络选择器获取用户身份信息，再结合步骤 15 用户选定的网络编号，在步骤 17 中一并通过 RJ45 Plus 的 T1、T2 发送给安全集线器。步骤 16 判定如果用户选择的网络号是 1~7，并且有本地硬盘的话，则在访问该计算机网络期

[redacted]硬盘的供电。这样可以防止将有密级的计算机网络信息卸载到该计算机的硬盘上，因为当该计算机再次访问互联网络时就有可能泄密。如果网络选择器没有用户身份卡，则将网络编号自动设为 0，意味着该用户只访问互联网，这就是步骤 14。步骤 18 等待安全集线器答复该用户的合法性，如果结论是不合法就进入到步骤 19，并停止该次连接入网。步骤 20 是网络选择器静观用户是否改变身份或网络号码，即是不是换了用户，如果没有换用户的话，当前用户是不是要改变所连接的计算机网络，有任何一个变动就到达 21 和 17，循环回来。

在图 10 中，步骤 41 是安全集线器通过 RJ45 Plus 的 T1、T2 等待来自网络选择器的请求，当没有请求时，循环等待，有请求时，进入步骤 42，这时一定是网络号或用户身份改变，如果是用户身份改变，但有权访问当前的计算机网络，则退出上一个用户的网络，为当前用户接通所要访问的计算机网络，这就是步骤 43、46、47，然后回到 41 等待；如果是用户身份改变，但无权访问当前计算机网络，则进入步骤 45，终止连接并向网络选择器报错。如果用户身份没有改变，那肯定是改变网络号了，44 如果用户有权限访问该计算机网络的话，步骤 48 通知当前文件服务器保留工作现场，根据用户身份、网络号码等连接到相应的新计算机网络的文件服务器，又回到 41。

由于八个计算机网络相互隔离，它们之间的数据不会被互相读取，特别地，从互联网络无法攻击其余的七个网络。因为无盘计算机接入八个计算机网络中的某个就自动成为该计算机网络的一部分，由于无硬盘，无法在本机保存数据，而有盘计算机访问带密级的计算机网络时，硬盘不工作，所以计算机不会因其退出网络再接入另一个网络时而泄露原有网络的信息，从而保障计算机网络的信息安全。

每当用户在不同密级的计算机网络之间切换时，网络服务器自动地保留用户的运行现场，以便再次切换回来时继续运行。

我们不妨更直观地审视实现这一方法的过程。该过程相当于在用户面

[redacted]在有几个互不相通的计算机网络时，用户根据需要把一台计算机的网络插头在各计算机网络之间插来插去。

之所以要用无盘的计算机，就是为了不从用户的计算机上泄露信息。之所以用网络选择器和安全集线器，是为了加长插插头的手的长度，同时减少布线和施工的成本。

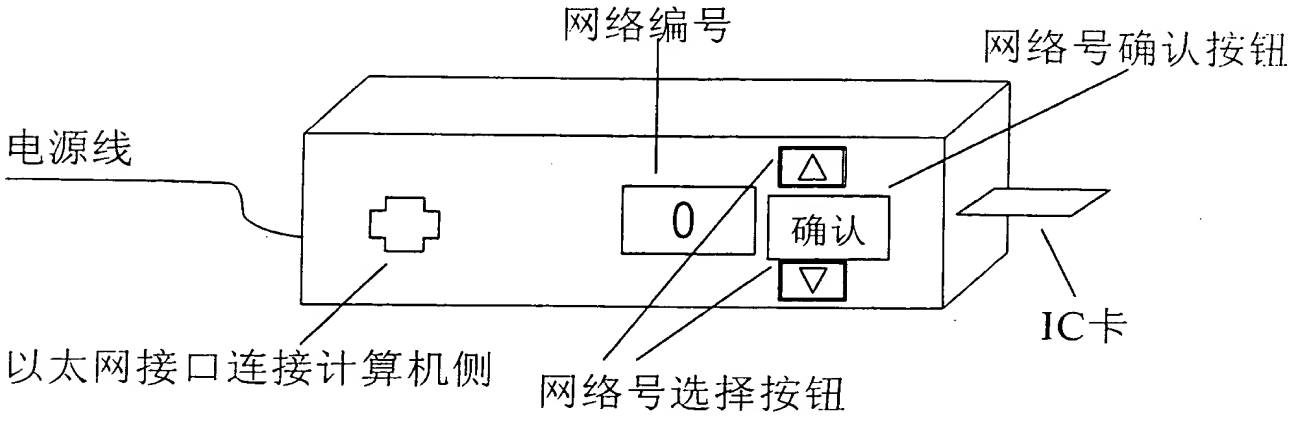
网络编号
网络号确认按钮
电源线
0
确认
IC卡
以太网接口连接计算机侧
网络号选择按钮

图1

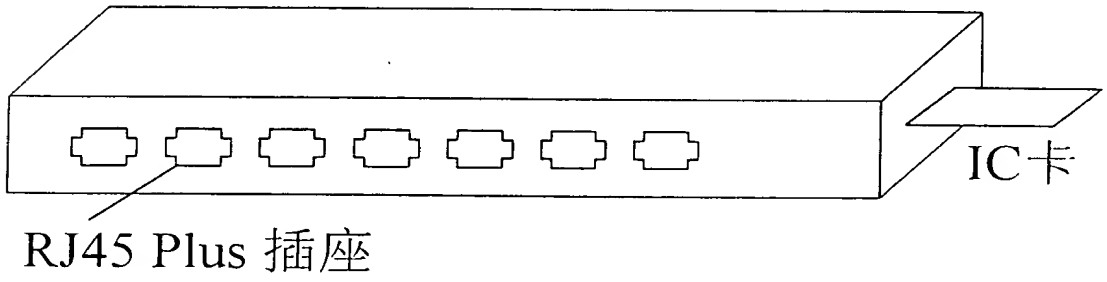
IC卡
RJ45 Plus 插座

图2

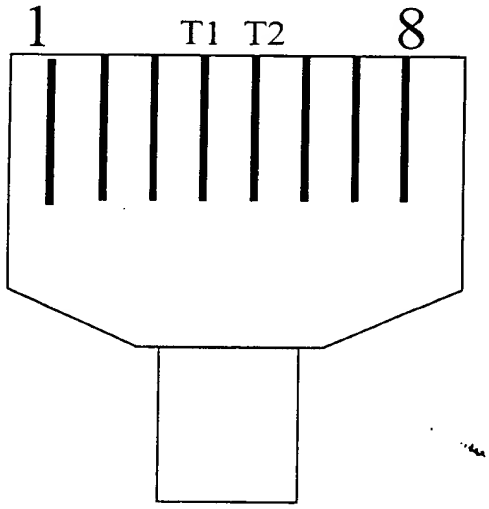
1
T1
T2
8

图3

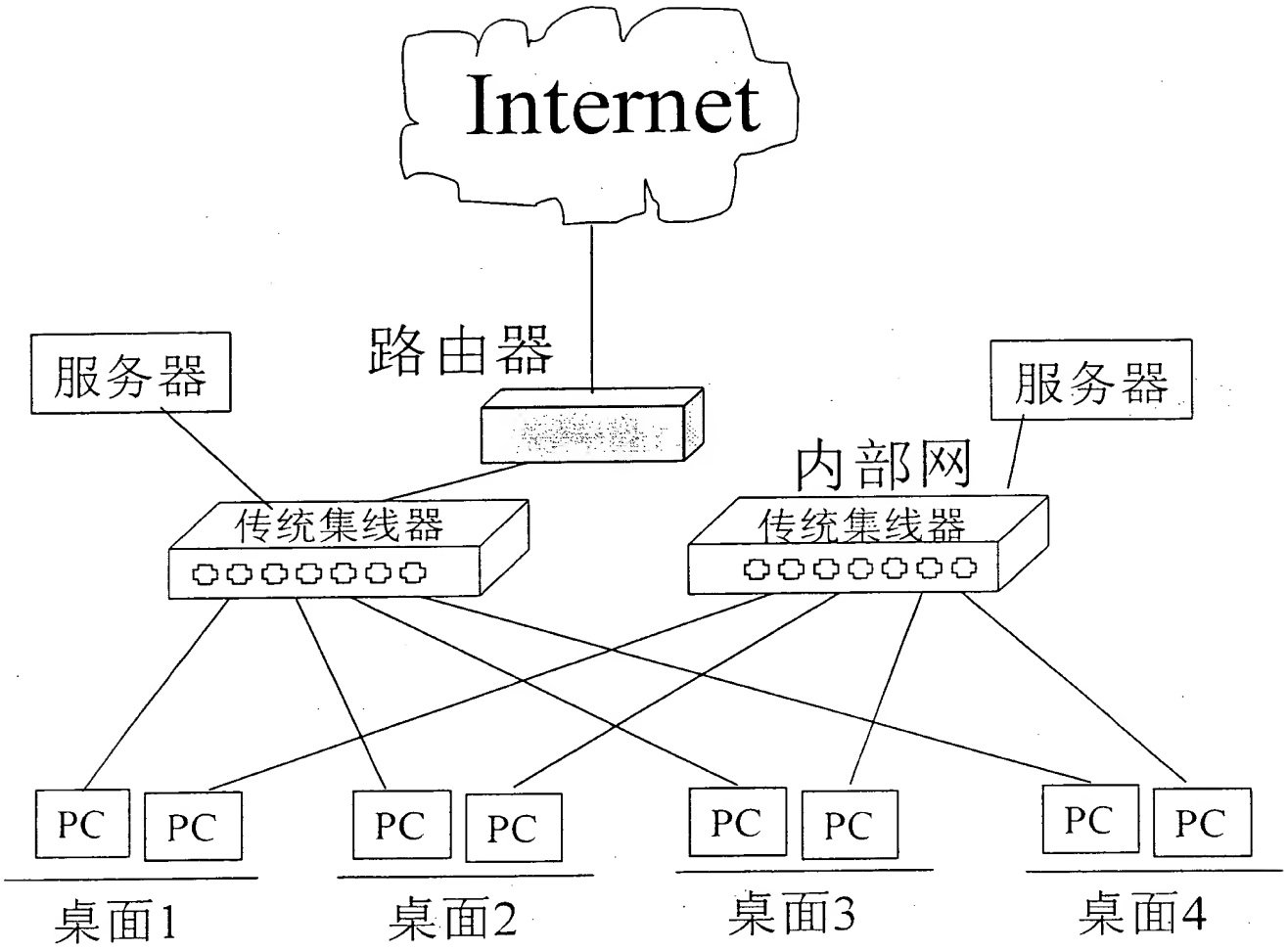
Internet
路由器
服务器
服务器
内部网
传统集线器
传统集线器
PC
PC
PC
PC
PC
PC
PC
PC
桌面1
桌面2
桌面3
桌面4

图4

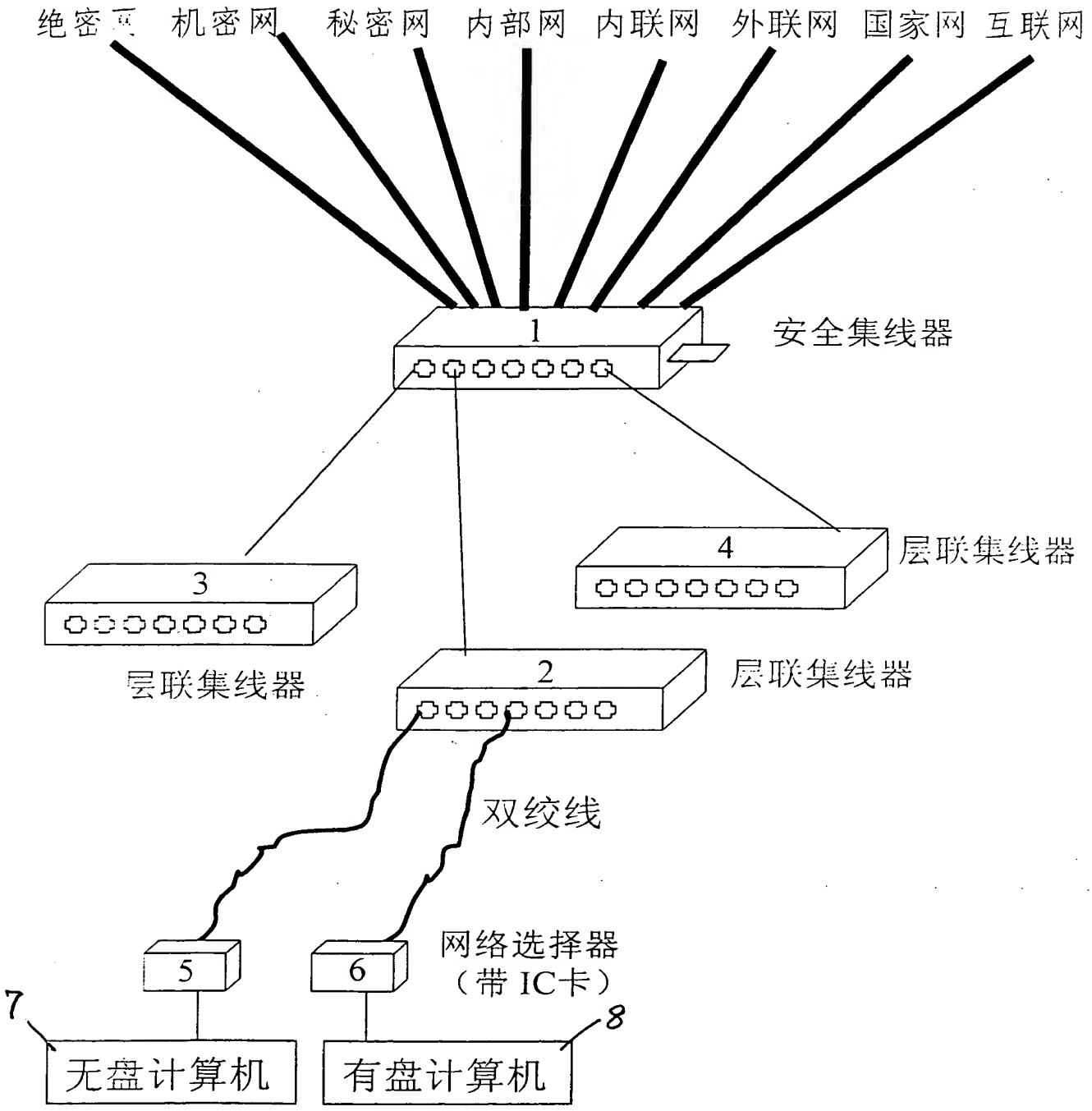
绝密网
机密网
秘密网
内部网
内联网
外联网
国家网
互联网
1
安全集线器
4
层联集线器
3
层联集线器
2
层联集线器
双绞线
5
6
网络选择器
（带 IC卡）
7
8
无盘计算机
有盘计算机

图5

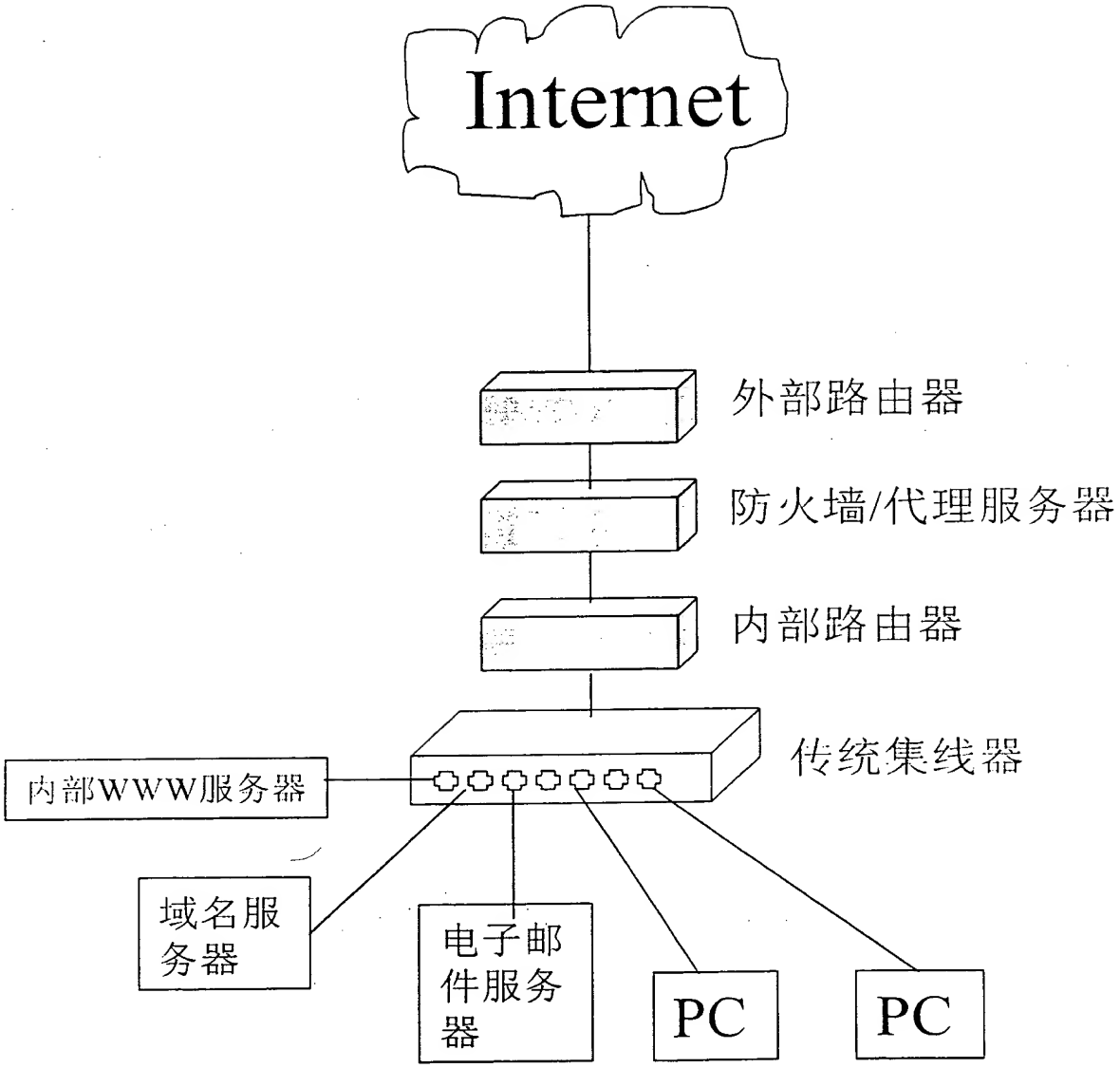
Internet
外部路由器
防火墙/代理服务器
内部路由器
传统集线器
内部WWW服务器
域名服务器
电子邮件服务器
PC
PC

图6

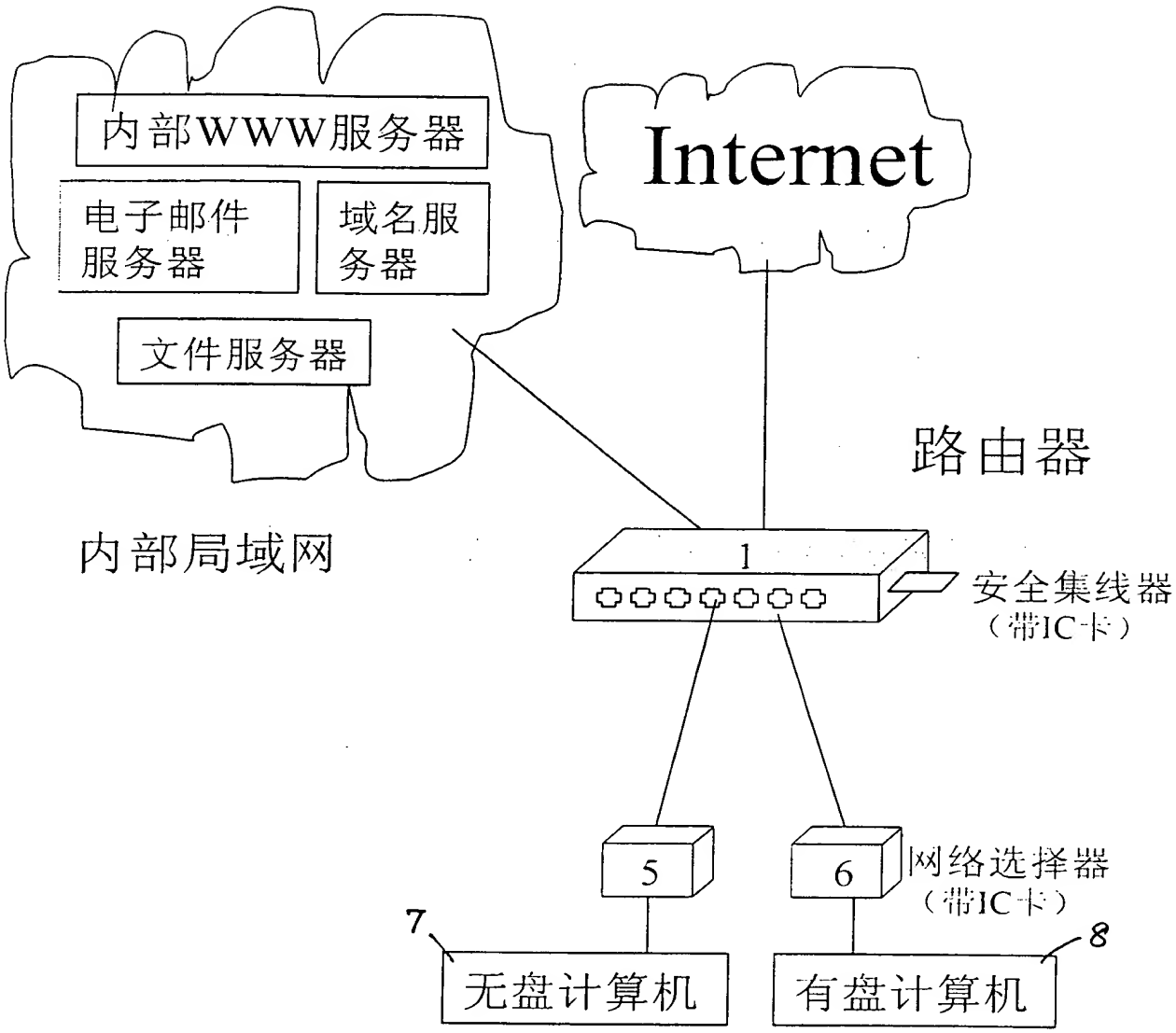
内部WWW服务器
电子邮件服务器
域名服务器
文件服务器
Internet
路由器
内部局域网
1
安全集线器
（带IC卡）
5
6
网络选择器
（带IC卡）
7
8
无盘计算机
有盘计算机

图7

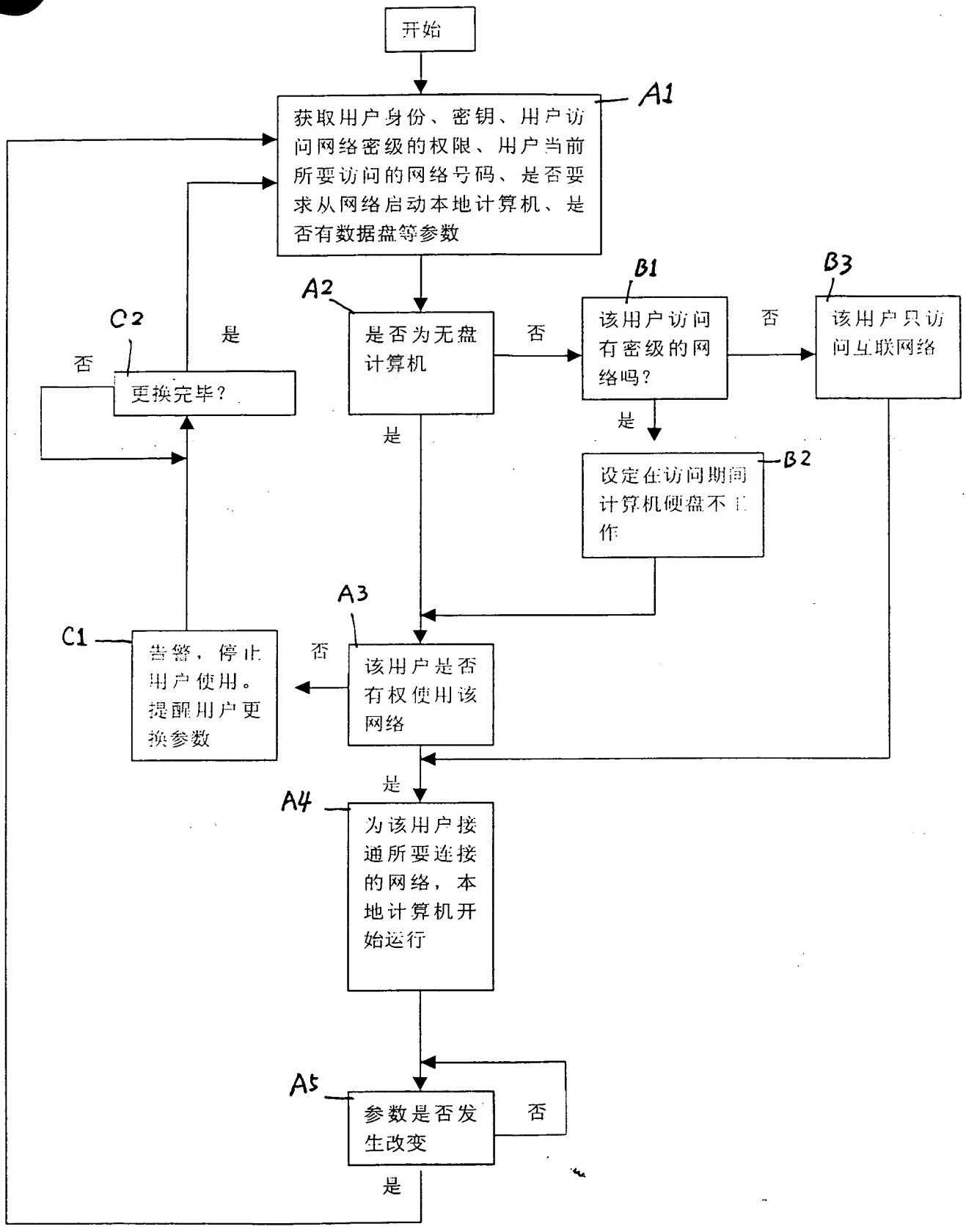
开始
A1
获取用户身份、密钥、用户访问网络密级的权限、用户当前所要访问的网络号码、是否要求从网络启动本地计算机、是否有数据盘等参数
A2
是否为无盘计算机
否
是
B1
该用户访问有密级的网络吗？
否
是
B3
该用户只访问互联网络
B2
设定在访问期间计算机硬盘不工作
C2
否
是
更换完毕？
A3
C1
否
告警，停止用户使用。提醒用户更换参数
该用户是否有权使用该网络
是
A4
为该用户接通所要连接的网络，本地计算机开始运行
A5
参数是否发生改变
否
是

图 8

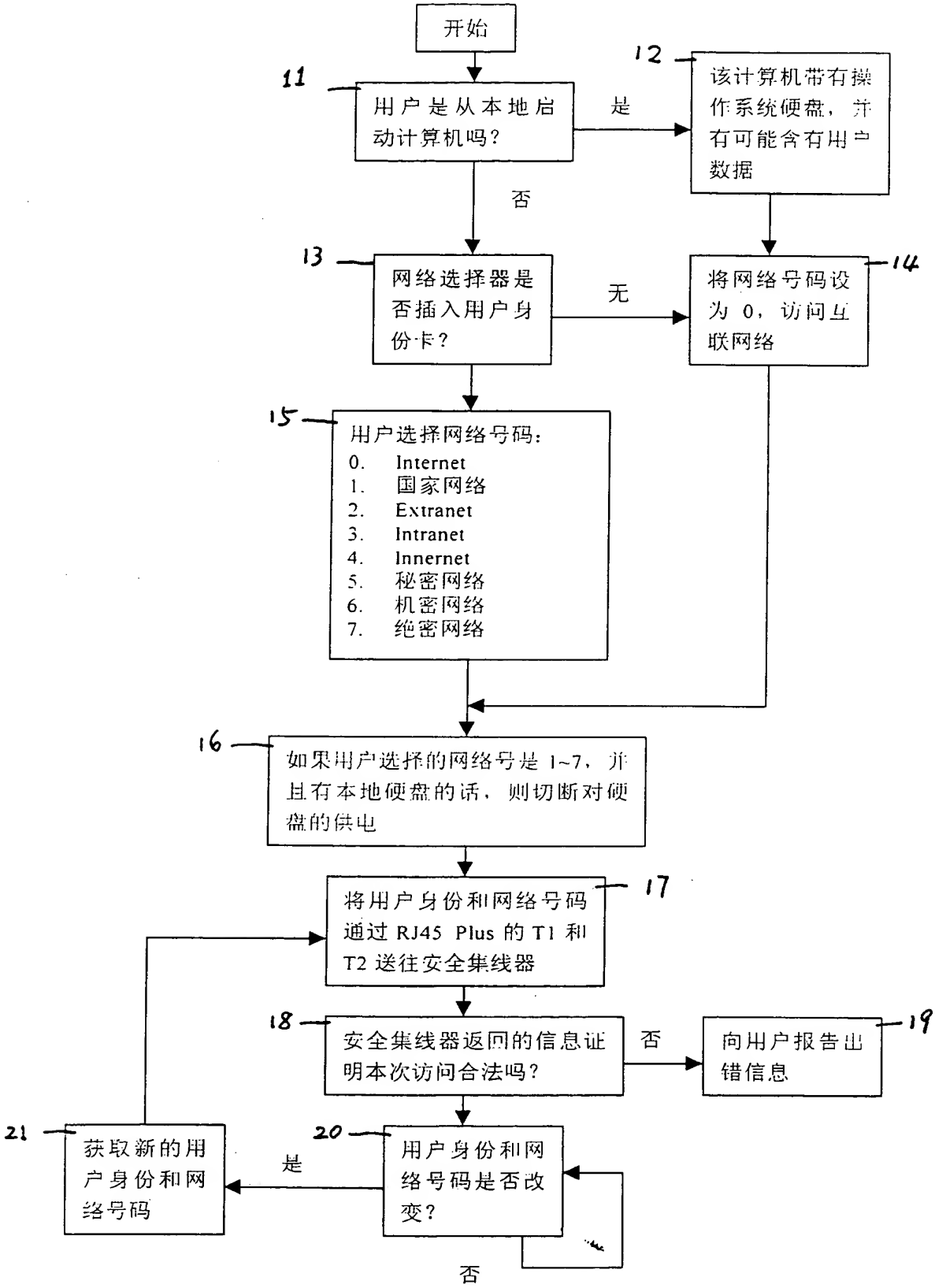
开始
11
用户是从本地启动计算机吗？
是
12
该计算机带有操作系统硬盘，并有可能含有用户数据
否
13
网络选择器是否插入用户身份卡？
无
14
将网络号码设为 0，访问互联网络
15
用户选择网络号码：
0. Internet
1. 国家网络
2. Extranet
3. Intranet
4. Innernet
5. 秘密网络
6. 机密网络
7. 绝密网络
16
如果用户选择的网络号是 1~7，并且有本地硬盘的话，则切断对硬盘的供电
17
将用户身份和网络号码通过 RJ45 Plus 的 T1 和 T2 送往安全集线器
18
安全集线器返回的信息证明本次访问合法吗？
否
19
向用户报告出错信息
20
用户身份和网络号码是否改变？
是
21
获取新的用户身份和网络号码
否

图 9

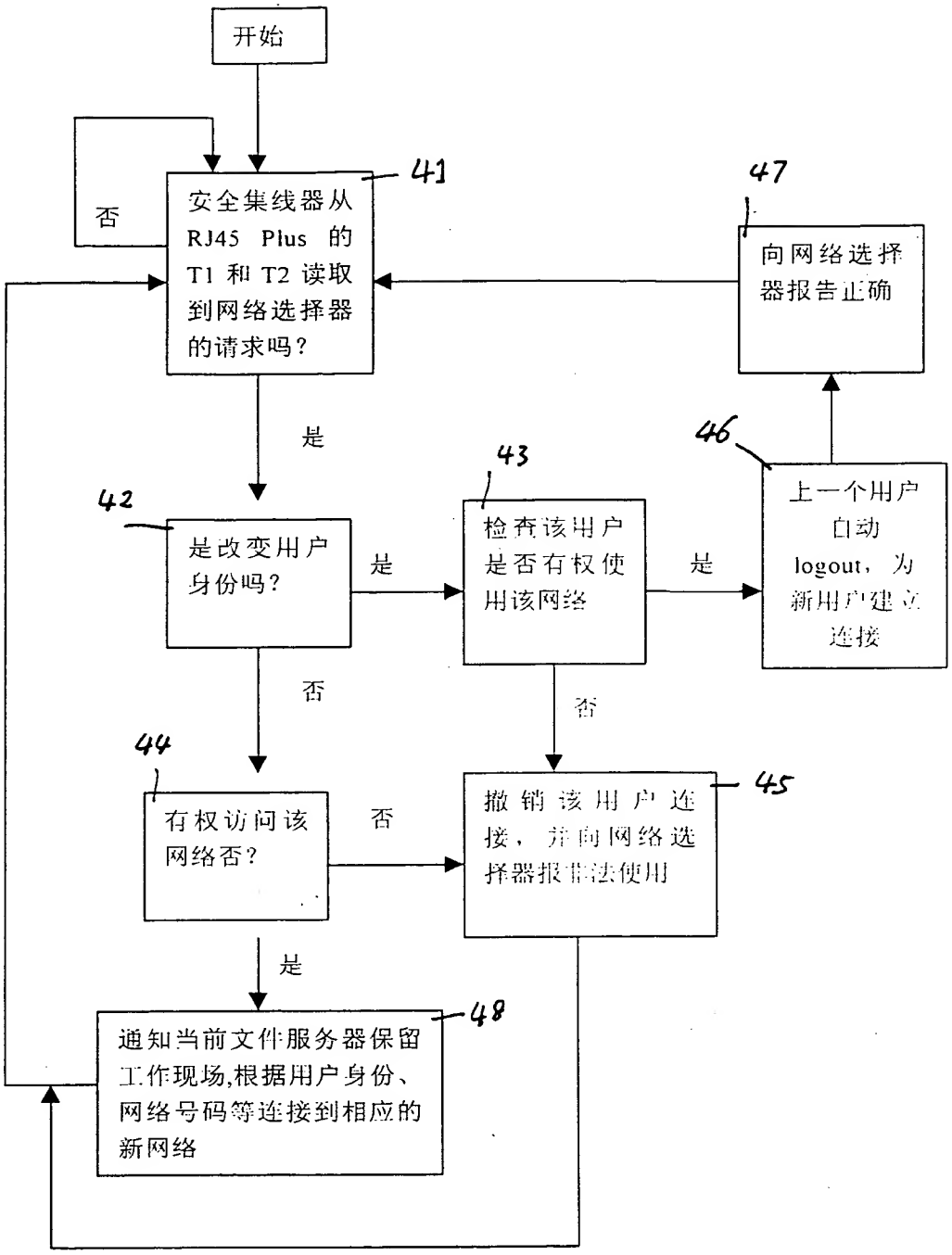
开始
41
安全集线器从 RJ45 Plus 的 T1 和 T2 读取到网络选择器的请求吗？
否
是
47
向网络选择器报告正确
46
上一个用户自动 logout，为新用户建立连接
43
检查该用户是否有权使用该网络
是
42
是改变用户身份吗？
是
否
否
44
有权访问该网络否？
否
45
撤销该用户连接，并向网络选择器报告无法使用
是
48
通知当前文件服务器保留工作现场,根据用户身份、网络号码等连接到相应的新网络

图 10